COMPSCI 314 S1 C

Data Communications Fundamentals

Lecture Slides, Set #5

Clark Thomborson
7 April 2006

IPsec

- There are two main parts to the IP security protocol:
  - IKE, the Internet Key Exchange, to set up keys
  - ESP/AH, the Encapsulating Security Payload and Authentication Header.
  - (ESP is *not* the "Encryption Security Payload" ;-)
- This is a very complex protocol: "over-engineered"?
  - RFC 2401 gives a 66 pp. overview (obsoleted by RFC 4301, December 2005, 99 pp.).
  - RFC 2402 defines AH; was obsoleted by RFC 4302 (33 pp.) and RFC 4305 (5 pp.)
  - Also: RFC 2403, RFC 2404, RFC 2405, RFC 2410, RFC 2411, RFC 4109, RFC 4306 …
  - See http://rfc.net/rfc-index.html.

RFC 2410: "The NULL Encryption Algorithm and Its Use With IPsec"

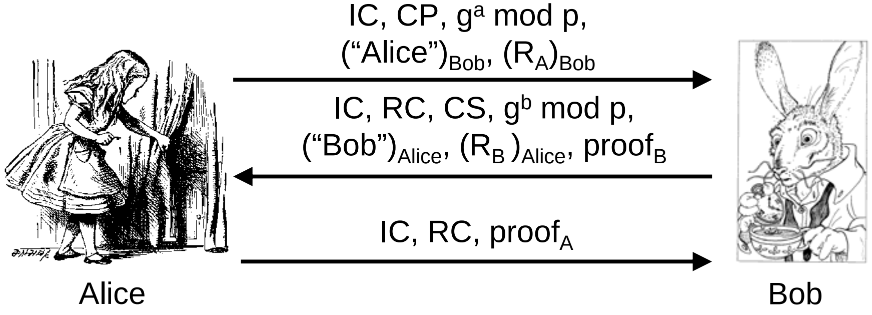
- "… NULL is a block cipher the origins of which appear to be lost in antiquity.
- "Despite rumors that the National Security Agency suppressed publication of this algorithm, there is no evidence of such action on their part.
- "Rather, recent archaeological evidence suggests that the NULL algorithm was developed in Roman times, as an exportable alternative to Ceaser [sic] ciphers.
- "However, because Roman numerals lack a symbol for zero, written records of the algorithm's development were lost to historians for over two millennia.
- "NULL is defined mathematically by the use of the Identity function I applied to a block of data b such that:

  NULL(b) = I(b) = b
- "Like other modern ciphers, e.g., RC5 [RFC-2040], the NULL encryption algorithm can make use of keys of varying lengths. However, no measurable increase in security is afforded by the use of longer key lengths."

Internet Key Exchange (IKE)

- There are two phases:
  - Phase 1: set up an IKE "security association". Four options:
    - Public key encryption (original)
    - Public key encryption (improved)
    - Digital signature (for use when Alice doesn't initially know Bob's public key)
    - Symmetric Key
    - For each of these options there is a "main mode" (6 messages) and an "aggressive mode" (3 messages, no anonymity for Bob or Alice except in public key options). Eight versions!!
  - Phase 2: set up an IPsec "security association"
    - This is a 3-message key-exchange.
- Source: M Stamp, *Information Security: Principles and Practice*, Wiley, 2006.

IKE PK, Aggressive Mode



IC, CP, g^a mod p, (“Alice”)$_{\text{Bob}}$, $(R_A)_{\text{Bob}}$

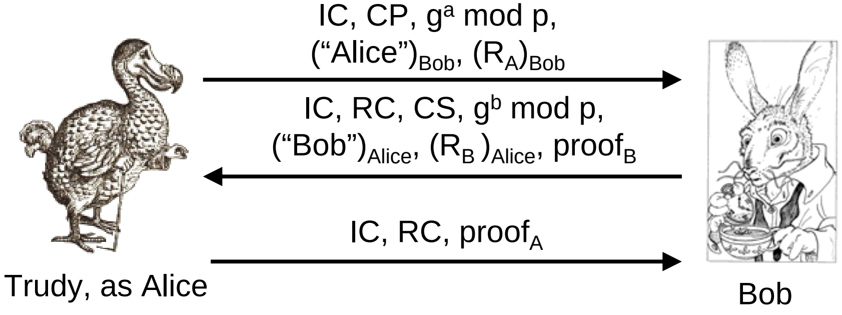
IC, RC, CS, g^b mod p, (“Bob”)$_{\text{Alice}}$, $(R_B)_{\text{Alice}}$, proof$_B$

IC, RC, proof$_A$

IC = initiator cookie, CP = crypto proposed,
CS = crypto selected, RC = responder cookie,
SKEYID = h(R_A, R_B, g^{ab} mod p),
proof$_A$ = [h(SKEYID, g^a mod b, g^b mod p, IC, RC, CP, “Alice”)]$_{\text{Alice}}$

Source: M Stamp, *Information Security: Principles and Practice*, Wiley, 2006.

Aggressive IKE PK is anonymous (!)



IC, CP, g^a mod p, (“Alice”)$_{\text{Bob}}$, $(R_A)_{\text{Bob}}$

IC, RC, CS, g^b mod p, (“Bob”)$_{\text{Alice}}$, $(R_B)_{\text{Alice}}$, proof$_B$

IC, RC, proof$_A$

IC = initiator cookie, CP = crypto proposed,
CS = crypto selected, RC = responder cookie,
SKEYID = h(R_A, R_B, g^{ab} mod p),
proof$_A$ = [h(SKEYID, g^a mod b, g^b mod p, IC, RC, CP, “Alice”)]$_{\text{Alice}}$

Source: M Stamp, *Information Security: Principles and Practice*, Wiley, 2006.

- This is called “plausible deniability” in IKE.
- Alice can deny sending messages to Bob: “Trudy did it!”

IPsec cookies

- The IC and RC cookies are called “anti-clogging tokens” in the relevant RFCs.
- These are unrelated to web cookies, which maintain state in a web browser.
- The IC and RC cookies are intended to allow Bob to remain stateless as long as possible during a session initiation.
  - In a typical DoS (denial-of-service) attack, Bob is overwhelmed by a flood of spurious requests for session initiations.
  - Bob will run out of memory if he tries to remember all session initiations that haven’t yet completed.
- Bob must remember CP from the first IKE message, when responding to the third message.
  - Bob is susceptible to DoS attacks on IKE initiations.

Source: M Stamp, *Information Security: Principles and Practice*, Wiley, 2006.

IPsec datagrams

- An IPsec datagram is protected by one of two protocols.
  - ESP (the Encapsulating Security Payload) protects integrity and confidentiality.
  - AH (the Authentication Header) protects integrity.
  - Everything beyond the IP header is protected.
- IPsec defines two transport modes.
  - In transport mode, the new ESP/AH header is sandwiched between the IP header and the data.
  - In tunnel mode, the entire IP packet is encapsulated in a new IP packet.

Source: M Stamp, *Information Security: Principles and Practice*, Wiley, 2006.

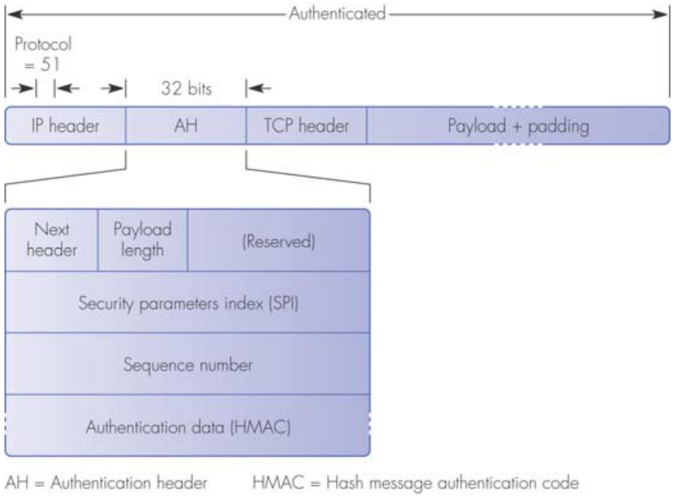
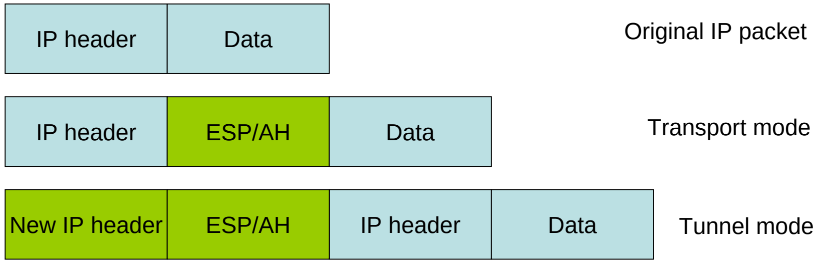

Authenticated
Protocol = 51
32 bits
IP header
AH
TCP header
Payload + padding
Next header
Payload length
(Reserved)
Security parameters index (SPI)
Sequence number
Authentication data (HMAC)
AH = Authentication header
HMAC = Hash message authentication code

Figure 10.15 AH protocol header position and contents in transport mode

What can an attacker learn by analysing this packet?

Transport Mode vs. Tunnel Mode



Source: M Stamp, *Information Security: Principles and Practice*, Wiley, 2006.

- Transport mode adds less header information:
  - more efficient.
- Tunnel mode with ESP doesn’t let the attacker see the IP header.
  - Firewall-to-firewall packets don’t reveal intranet addresses.
  - The attacker can see firewall (internet) addresses in the new IP header.

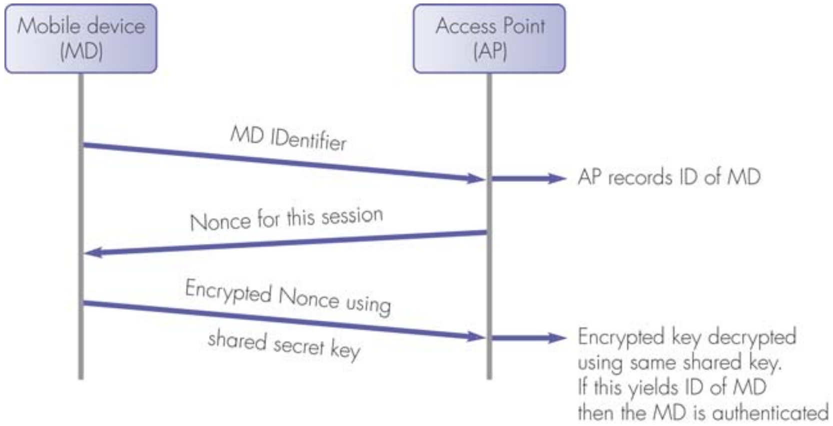

Mobile device (MD)
Access Point (AP)
MD IDentifier
AP records ID of MD
Nonce for this session
Encrypted Nonce using shared secret key
Encrypted key decrypted using same shared key. If this yields ID of MD then the MD is authenticated

Figure 10.17 Authentication of a mobile device by the AP using a three-way handshake procedure

Has the AP authenticated itself to the MD?

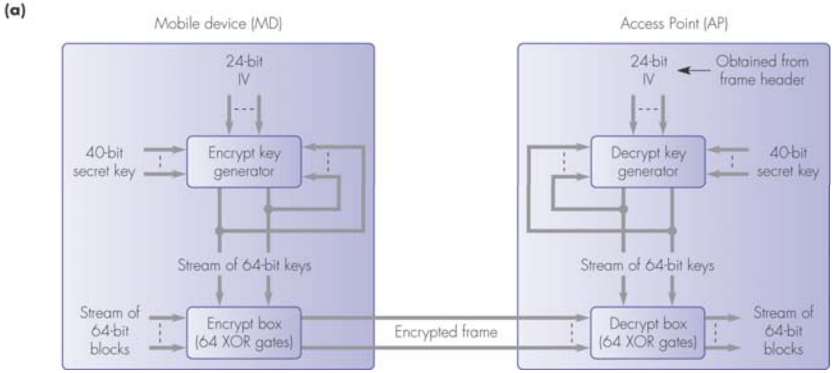


Figure 10.18 WEP protocol: (a) RC4 stream cipher principles

Note that the IV is sent “in the clear”! Eavesdropper can see when the same IV is used twice => same stream cipher => enables a cryptographic attack on RC4.

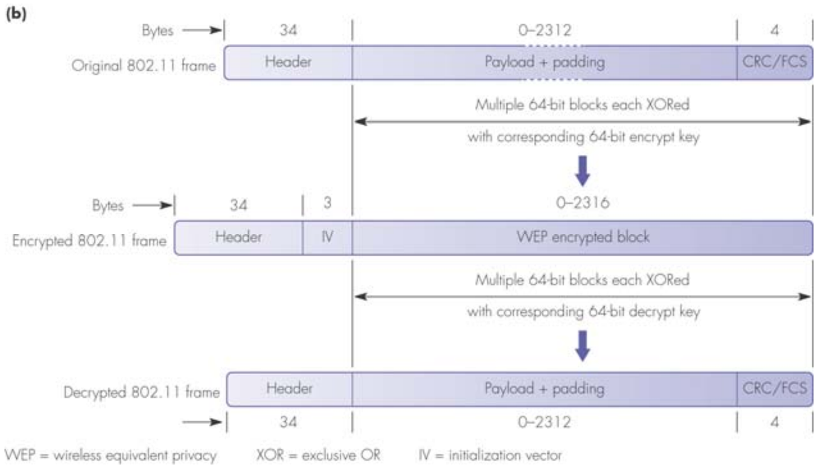


Figure 10.18 WEP protocol: (b) frame encryption/decryption operations

Note use of CRC: a poor choice with XOR (stream cipher), allows modification attacks.

In(Security) of the WEP Algorithm

- A busy access point, which constantly sends 1500 byte packets at 11Mbps, will exhaust the space of IVs after 1500*8/(11*10^6)*2^24 = ~18000 seconds, or 5 hours.
  - The amount of time may be even smaller, since many packets are smaller than 1500 bytes.
- This allows an attacker to collect two ciphertexts that are encrypted with the same key stream and perform statistical attacks to recover the plaintext.
- Worse, when the same key is used by all mobile stations, there are even more chances of IV collision.
  - For example, a common wireless card from Lucent resets the IV to 0 each time a card is initialized, and increments the IV by 1 with each packet.
  - This means that two cards inserted at roughly the same time will provide an abundance of IV collisions for an attacker.
- Source: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2001.

802.11g, 802.11i, …

- 802.11g: defines Wi-Fi Protected Access (WPA).
  - Ratified as a standard in June 2003.
  - Includes some of the security improvements in a draft of 802.11i.
- 802.11i: defines WPA2.
  - Ratified in June 2004.
  - Uses the Advanced Encryption Standard (AES), instead of RC4, which was used in WEP and WPA.
- 802.11w: protect management and broadcast frames.
  - Task group started work in January 2005.
  - Target date for ratification: March 2008.
- Sources:
  - http://en.wikipedia.org/wiki/802.11 (23:30, 4 April 2006),
  - http://en.wikipedia.org/wiki/IEEE_802.11w (07:14, 7 March 2006).

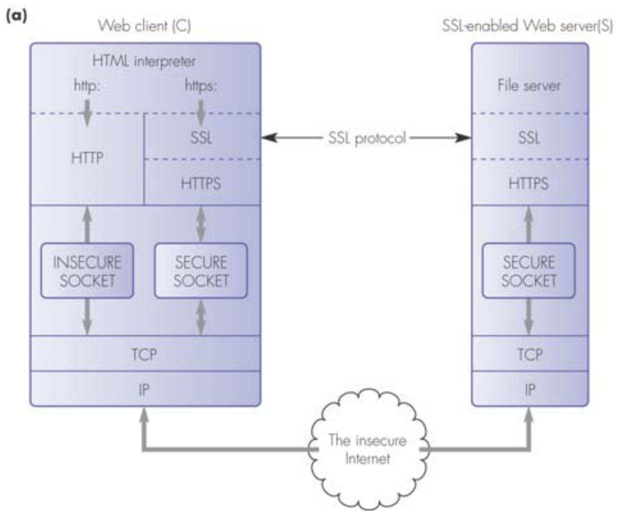
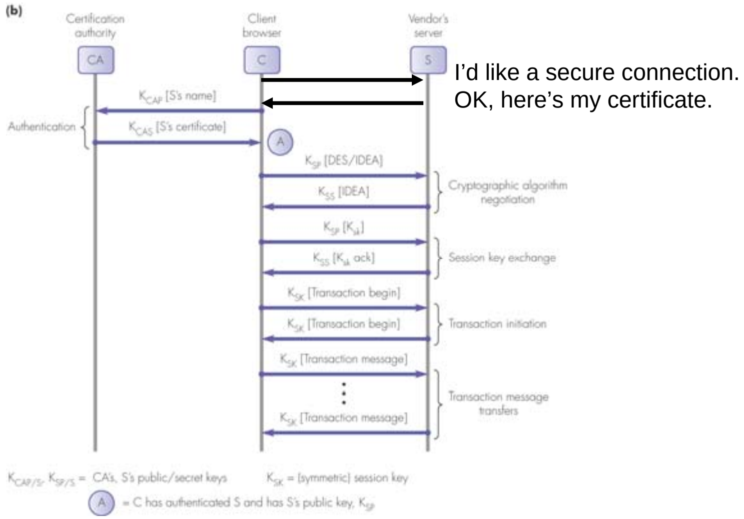


Figure 10.19 The secure socket layer (SSL) protocol: (a) protocol stack

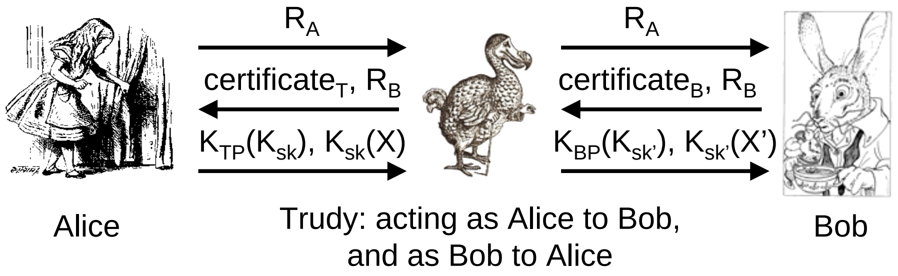

(b)
Certification authority
Client browser
Vendor's server
CA
C
S
K_{CAP} [S's name]
Authentication
K_{CAS} [S's certificate]
A
K_{SP} [DES/IDEA]
K_{SS} [IDEA]
Cryptographic algorithm negotiation
K_{SP} [K_{sk}]
K_{SS} [K_{sk} ack]
Session key exchange
K_{SK} [Transaction begin]
K_{SK} [Transaction begin]
Transaction initiation
K_{SK} [Transaction message]
K_{SK} [Transaction message]
Transaction message transfers
$K_{CAP/S}$, $K_{SP/S}$ = CA's, S's public/secret keys
K_{SK} = (symmetric) session key
A = C has authenticated S and has S's public key, K_{SP}

I'd like a secure connection.
OK, here's my certificate.

Figure 10.19 The secure socket layer (SSL) protocol: (b) outline of the authentication and transaction initiation phases

Does C authenticate to S? Does S authenticate to C? What if CA is offline?

SSL Protection against Man-in-the-Middle



R_A

certificate$_T$, R_B

$K_{TP}(K_{sk})$, $K_{sk}(X)$

R_A

certificate$_B$, R_B

$K_{BP}(K_{sk'})$, $K_{sk'}(X')$

Alice

Trudy: acting as Alice to Bob, and as Bob to Alice

Bob

- How can Alice detect that Trudy is "in the middle"?
- What does your web-browser do, when it receives an SSL certificate that is invalid?
  - Your browser has a collection of public keys for CAs.
- Have you ever inspected an SSL certificate?

Secure Electronic Transfer (SET)

- Developed by Visa & Mastercard, starting in 1996.
- Excellent cryptographic design, based on iKP family of protocols (i=1, 2, 3) from IBM R&D Zurich. Assurances:
  - Confidentiality (merchant doesn't learn customer's credit card number); Integrity;
  - Authentication of merchants (for i>1), and of customers (i=2).
  - Non-repudiability by merchants (for i>1), and by customers (i=2).
  - Source: Bellare et al., *IEEE J SAC 18:4* 611-627, April 2000.
- Failed to win market share. Visa now uses 3-D Secure.
  - For i=2, customers must have a public key certificate, e.g. on a smart-card. (A chicken-and-egg problem.)
  - Doesn't support e-commerce from home (smart-card reader expense).
  - Source: http://cs.bilkent.edu.tr/~selcuk/teaching/cs519/cs519.21.ppt
  - Some merchants use credit card numbers to recognize repeat customers. (A legacy-software problem.)

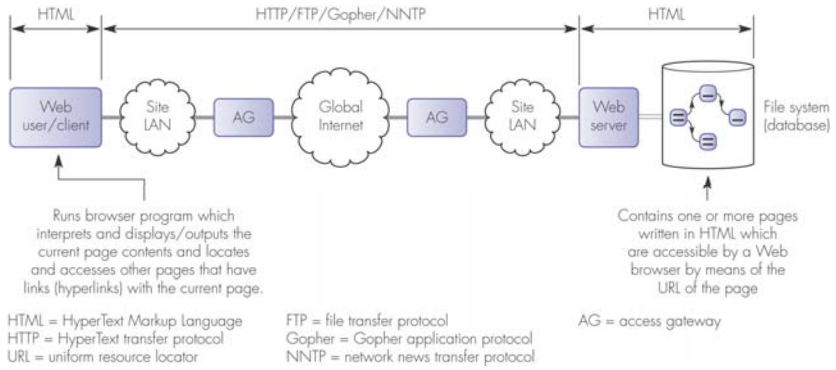

HTML
HTTP/FTP/Gopher/NNTP
HTML
Web user/client
Site LAN
AG
Global Internet
AG
Site LAN
Web server
File system (database)
Runs browser program which interprets and displays/outputs the current page contents and locates and accesses other pages that have links (hyperlinks) with the current page.
Contains one or more pages written in HTML which are accessible by a Web browser by means of the URL of the page
HTML = HyperText Markup Language
HTTP = HyperText transfer protocol
URL = uniform resource locator
FTP = file transfer protocol
Gopher = Gopher application protocol
NNTP = network news transfer protocol
AG = access gateway

Figure 9.1 Information browsing

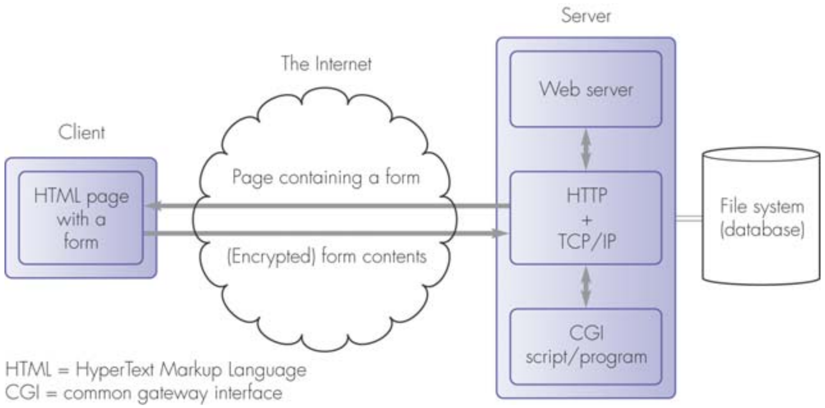


Figure 9.3 Electronic commerce

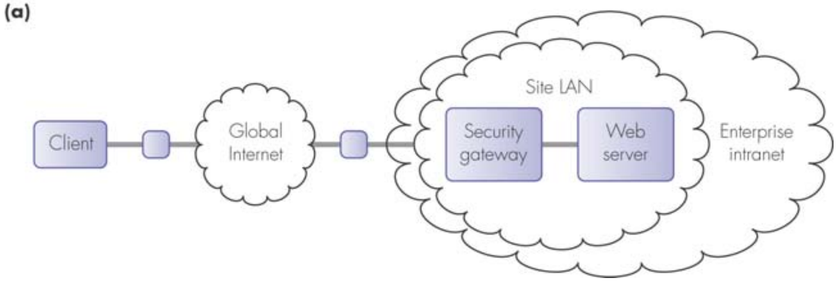


Figure 9.4 Intermediate systems: (a) security gateway

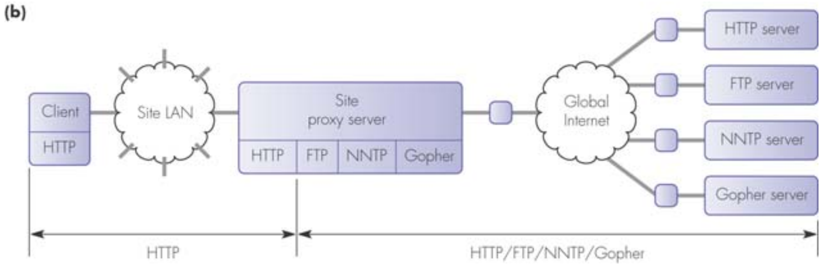


Figure 9.4 Intermediate systems: (b) proxy server

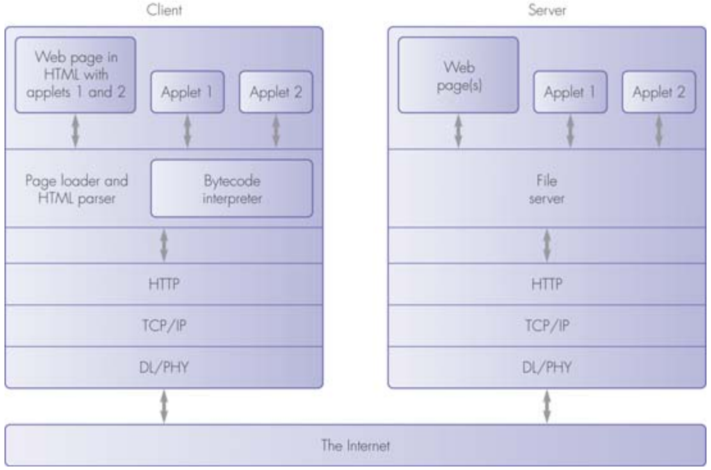


Figure 9.5 Protocol stack to support the browsing of pages containing Java applets